

Generalizing some properties of differential uniformity and non-linearity of permutations on finite commutative rings

Sonu Pal ^{*}
Anupama Panigrahi [†]
Department of Mathematics
University of Delhi
New Delhi 110007
Delhi
India

Saibal K. Pal [§]
Defence Research and Development Organization
Metcalfe House
New Delhi 110054
Delhi
India

Abstract

This study examines two essential characteristics of permutations within algebraic frameworks. The initial emphasis is on the full differential uniformity of permutations within a finite commutative ring possessing unity. We generalize the permutation results examined by Gupta, Mishra, and Gaur [10] in 2021 about $\mathbb{Z}_n$ to encompass broader finite commutative rings. Expanding upon the research conducted by Canteaut, Duval, and Leurent, [3] in 2015 about differential uniformity bounds for functions derived from Feistel and Misty architectures, we introduce novel bounds for functions formulated using Lai-Massey structures.

Subject Classification: 94A60, 11T71, 05A05.

Keywords: Full differential uniformity, Non linearity, Permutations, S-boxes, Lai-Massey structure.

^{*} ORCID-ID: 0009-0008-9199-9337

[†] ORCID-ID: 0000-0003-4637-3702

[§] ORCID-ID: 0000-0003-3297-1605

^{*} E-mail: sonupal923@gmail.com (Corresponding Author)

[†] E-mail: apanigrahi@maths.du.ac.in

[§] E-mail: skptech@yahoo.com

1. Introduction

Over the years, researchers have studied permutations over an algebraic structure. Proposing a robust cryptosystem is the major application of such functions. Some of the stream ciphers that use permutations are RC4 [20] and its variants, VPMC, VPMC-R [22], etc. Some block ciphers, like AES [8] and PRESENT [2], use permutations over the finite field of the form $\mathbb{F}_2^8$ and $\mathbb{F}_2^4$, respectively. A permutation's non-linearity and differential uniformity are two important cryptographic properties. Firstly, the concept of non-linearity was introduced simply using a Boolean function, and later the concept was extended to permutations [6, 7, 15].

Beth and Ding explored the non-linearity of Boolean functions within finite fields [1]. Following this, Carlet and Ding broadened the scope of their investigation to include finite Abelian groups [4]. A few years ago, Mishra and his colleagues introduced non-linearity over the ring of integer modulo n , $\mathbb{Z}_n$ [16]. Additionally, they also studied the non-linearity of k -cycle permutations [13] and affine equivalence of permutations over $\mathbb{Z}_n$ [12] respectively.

Gupta, Mishra, and Gaur [10, 17] recently investigated the differential uniformity of permutations on $\mathbb{Z}_n$. They provided some results on permutations over $\mathbb{Z}_n$ that exhibit full differential uniformity, as well as some bounds on the quantity of such permutations. In addition, they computed various bounds on the non-linearity of permutations over $\mathbb{Z}_n$ and established bounds for the maximum possible non-linearity attainable by a permutation, as stated in [11].

Beyond permutation-based constructions, recent cryptographic research has increasingly explored non-field algebraic structures, particularly rings, due to their potential to offer enhanced security and richer algebraic complexity. Selikh et al. [21] proposed an innovative cryptosystem founded over a non-commutative ring structure, demonstrating that ring-based frameworks can provide strong cryptographic primitives while introducing additional hardness assumptions compared to classical field-based systems. Similarly, Gowdhaman et al. [9] investigated constacyclic codes over the finite commutative ring $\mathbb{Z}_4[a, b]/\langle a^2 - a, b^2, ab \rangle$, highlighting the applicability of structured rings in coding theory and cryptography. These works further emphasize the relevance of algebraic constructions over rings and motivate the study of permutation characteristics such as differential uniformity and non-linearity in broader algebraic domains.

In our paper, we have extended the concept of full differential uniformity of permutation over $\mathbb{Z}_n$ to finite commutative ring with unity and also able to give an interconnection of differential uniformity and non-linearity of permutations within finite commutative rings. Motivated by the work done by authors in [3, 14] for giving lower bounds for the differential uniformity of function constructed using Feistel and Misty structures, we also give some bounds for the differential uniformity of function constructed using Lai-Massey structure.

Section 2 is devoted to showing the existence of some permutations exhibiting full differential uniformity over a general finite unital commutative ring. Some properties of full differential uniformity of permutation over $\mathbb{Z}_n$ have been extended to any finite unital commutative ring. In Section 3, we established

an interconnection between the non-linearity and differential uniformity of a permutation over ring R . Later, in Section 4, we provide a bound for the differential uniformity of a function constructed with 3 rounds of Lai-Massey structure. In the last, we conclude our work along with our future directions in Section 5.

1.1 Preliminaries

Throughout this article, unless specified otherwise, R refers to the finite commutative ring with unity. We will abbreviate the term commutative ring with unity by CRU. R^* signifies the collection of all unit elements within R . Additionally, for any element t in R , $|t|_+$ represents the additive order of t in the group $(R, +)$. The symbol $\lceil \cdot \rceil$ is used to denote the ceiling function. For any non-empty set Y , the symbol $|Y|$ denotes the cardinality of Y . Let S_Y denote the set of all permutations on a finite non-empty set Y . It forms a group structure (symmetric group on $|Y|$ symbols) under composition of functions. The number $d_H(h, k) = |Y| - |Eq(h, k)|$, where $Eq(h, k) = \{y \in Y | h(y) = k(y)\}$ represents Hamming distance between two permutations h and k on Y . This d_H forms a metric structure on S_Y as stated in [18]. The collection of all affine permutations on finite ring R is given by

$$\mathcal{A} = \{g(x) = rx + s, \forall x \in R | r \in R^*, s \in R\}.$$

The non-linearity of a permutation g on finite ring R [18] is denoted as $\mathcal{NL}(g)$ and is defined as

$$\mathcal{NL}(g) = \min_{l \in \mathcal{A}} d_H(g, l)$$

For $r, s \in R \setminus \{0\}$, we define $\delta_g(r, s)$ [1] as

$$\delta_g(r, s) = \{y \in R | g(y + r) - g(y) = s\}.$$

The differential uniformity of the above permutation $\Delta(g)$ [1, 19] is given as

$$\Delta(g) = \max_{r, s \in R \setminus \{0\}} |\delta_g(r, s)|.$$

Note that $1 \leq \Delta(g) \leq |R|$. A permutation with $\Delta(g) = 2$ is said to be an almost perfect nonlinear (APN) permutation [1]. An n -bit S-box, T is a mapping from $\mathbb{F}_2^n \mapsto \mathbb{F}_2^n$. The (u, v) differential of such functions is denoted as

$$\delta_T(u, v) = \{x \in \mathbb{F}_2^n | T(x) \oplus T(x \oplus u) = v\},$$

where $u \neq 0, v \in \mathbb{F}_2^n$. The differential uniformity of such function is defined as follows:

$$\Delta(T) = \max_{u \neq 0, v \in \mathbb{F}_2^n} |\delta_T(u, v)|.$$

Note that for every $0 \neq u \in \mathbb{F}_2^n$, the solution of the equation $T(x) \oplus T(x \oplus u) = v$ always exists in pairs. Thus, $2 \leq \Delta(T) \leq 2^n$.

2. Characteristics of permutations exhibiting full differential uniformity

In this section, we examine properties associated with permutations possessing full differential uniformity within a finite CRU. Note that in this section, whenever we talk about the non-linearity of a permutation on the finite ring R , we are considering the definition defined by the authors in [18]. Initially, we explore the presence of such permutations in a broad context of finite CRU. An immediate example of such permutation is the identity permutation on any finite CRU. Our next result provide a broader range of such permutations.

Proposition 2.1: The differential uniformity of every affine permutation over a finite CRU R is equal to the cardinality of R .

Proof: Let $|R| = n$, where R is a CRU, and f is an affine permutation. Thus,

$$f(y) = ay + b,$$

for some $a \in R^*$ and $b \in R$. Then for any $b_1 \neq 0$, we can choose $a_1 = a^{-1}b_1$ such that

$$|\{y \in R | f(y + a_1) - f(x) = b_1\}| = n.$$

Hence $\Delta(f) = n$.

Note that these are not the only permutations that possess full differential uniformity, as shown by the following example.

Example 2.2: Let $f = (2,4)(3,5)$ be a permutation in $\mathbb{Z}_6$. By exhaustive search, we get $\Delta(f) = |\delta_f(2,4)| = 6$. Alternatively, since f satisfies the conditions of [17, Theorem 1] and hence $\Delta(f) = 6$. It is easy to verify that f is a non-affine permutation with two fixed points, and hence $2 \leq \mathcal{NL}(f) \leq 4$.

Some properties of permutations exhibiting full differential uniformity over a finite CRU are given below.

Proposition 2.3: Let g be a permutation over a finite CRU R , such that

$$\Delta(g) = n = |R| = |\delta_g(r, s)|,$$

then the following holds;

1. $|r|_+ = |s|_+$.
2. If $|r|_+ = |s|_+ = n$, then g is an affine permutation.

Proof:

1. Let $|r|_+ = k < n$, then there exist an additive subgroup $K \subset R$ of additive group R such that

$$K = \{0, r, 2r, \dots, (k-1)r\}.$$

Since $\Delta(g) = n = |\delta_g(r, s)|$, therefore the equation $g(x + r) - g(x) = s$ has exactly n solutions in R . This implies that

$$\begin{aligned}
g(r) - g(0) &= s \\
g(2r) - g(r) &= s \\
&\vdots = \vdots \\
g(kr) - g((k-1)r) &= s
\end{aligned}$$

Adding all the above equations, we get $g(kr) - g(0) = ks$. This implies that, $ks = 0$. Suppose, if possible, $|s|_+ = p < k$, then adding the first p equations gives us $ps = g(pr) - g(0)$, which implies that $pr = 0$, a contradiction to the fact that $|r|_+ = k$. Hence, $|s|_+ = k$.

2. Let $|r|_+ = |s|_+ = n$, then $R = \{0, r, 2r, \dots, (n-1)r\}$. Since $\Delta(g) = n$, this gives

$$\begin{aligned}
g(r) - g(0) &= s \\
g(2r) - g(r) &= s \\
&\vdots = \vdots \\
g(nr) - g((n-1)r) &= s.
\end{aligned}$$

Note that by adding first k equations for $k \leq n$, we get

$$ks = g(kr) - g(0).$$

Now, for any $x, y \in R$

$$x = l_1 r \text{ and } y = l_2 r,$$

where $0 \leq l_1, l_2 \leq n-1$. Then

$$\begin{aligned}
g(x+y) &= g((l_1 + l_2)r) \\
&= (l_1 + l_2)s + g(0) \\
&= l_1 s + l_2 s + g(0) \\
&= g(x) + g(y) - g(0)
\end{aligned}$$

and hence g is an affine permutation.

Corollary 2.4: Let f be a permutation in a CRU R and R contains exactly p elements, where p is a prime. Then $\mathcal{NL}(f) = 0$.

Proof: The proof is immediate by applying the last proposition and Lagrange's theorem.

A natural lower bound on the quantity of permutations with full differential uniformity over the ring R is $|\mathcal{A}| = |R||R^*|$, that is, $|F_{|R|}| \geq |R||R^*|$ where $|F_{|R|}|$ is the number of permutations with differential uniformity equal to $|R|$.

Proposition 2.5: Let g be a permutation over a finite CRU R and $l, r \in R$, then

$$|\delta_g(l, r)| = |\delta_g(-l, -r)|,$$

where $-l$ and $-r$ denote the additive inverse of l and r , respectively.

Proof: Define a function $\phi: \delta_g(l, r) \mapsto \delta_g(-l, -r)$ as $\phi(y) = y + l$. Let $y \in \delta_g(l, r)$, that is, $y \in R$, and satisfy the equation

$$g(y + l) - g(y) = r,$$

then

$$g(y) - g(y + l) = -r.$$

$g(y + l - l) - g(y + l) = -r$, that is, $t = y + l \in \delta_g(-l, -r)$. Hence, this function is a well-defined function. Clearly, this map is injective. For the surjection, pick any $t \in \delta_g(-l, -r)$. Then $y = t - l \in \delta_g(l, r)$ such that $\phi(y) = t$. This proves the bijection of ϕ and gives $|\delta_g(l, r)| = |\delta_g(-l, -r)|$.

3. An interconnection between non-linearity and differential uniformity on finite CRU R .

Firstly, an interconnection of non-linearity and differential uniformity of permutation over the finite CRU R is given in this section. Later, we explored some lower bounds of differential uniformity of $2n$ -bit function ϕ which is constructed using three-round Lai-Massey structure with three internal n -bit S-boxes T_1 , T_2 , and T_3 .

Theorem 3.1: *Let g be a permutation on finite CRU R , where $|R| = m \geq 2$. Then the following holds:*

- (a) If $\mathcal{NL}(g) = L$, then $\Delta(g) \geq \left\lceil \frac{(m-L)(m-L-1)}{m-1} \right\rceil$.
- (b) If $\Delta(g) = D$, then $\mathcal{NL}(g) \geq \left\lceil m - \frac{1}{2} - \sqrt{(m-1)D + \frac{1}{4}} \right\rceil$.

Proof:

- (a) Let $\mathcal{NL}(g) = L = m - \max_{I \in \mathcal{A}} |Eq(g, I)|$. So there exists a permutation $I \in \mathcal{A}$ such that $I(x) = rx + s$ and $|Eq(g, I)| = m - L = k$ (say), where $r \in R^*$ and $s \in R$.

Let

$$\begin{aligned} E = Eq(g, I) &= \{d \in R | g(d) = I(d)\} \\ &= \{d \in R | g(d) = rd + s\}. \end{aligned}$$

Note that $|E| = k$. Let $Z \subset E \times E$ such that

$$Z = \{(a, b) \in E \times E | a \neq b\}.$$

Note that $|Z| = k(k-1)$. Now, we define a map $\psi: Z \rightarrow R \setminus \{0\}$ as

$$\psi(a, b) = a - b.$$

Clearly, this map is well defined as $a \neq b$. Also, there exists an element $\lambda \in R \setminus \{0\}$ that has at least v preimages, where $v = \left\lceil \frac{k(k-1)}{(m-1)} \right\rceil$.

Consequently,

$$\begin{aligned} v &\leq |\{(d_1, d_2) \in Z | \psi(d_1, d_2) = \lambda\}| \\ &= |\{(d_1, d_2) \in Z | d_1 - d_2 = \lambda\}| \\ &= |\{d_2 \in E | d_2 + \lambda \in E\}| \\ &= |\{d_2 \in R | g(d_2) = rd_2 + s \text{ \& } g(d_2 + \lambda) = r(d_2 + \lambda) + s\}| \\ &\leq |\{d_2 \in R | g(d_2 + \lambda) - g(d_2) = r\lambda\}| = |\delta(r, r\lambda)|. \end{aligned}$$

Thus, $v \leq |\delta(r, r\lambda)| \leq \Delta(g)$, that is,

$$\Delta(g) \geq \left\lceil \frac{(m-L)(m-L-1)}{m-1} \right\rceil. \quad (1)$$

Let D be the differential uniformity of g , and L denotes the non-linearity of permutation g . Then, by equation (1), $D \geq \left\lceil \frac{(m-L)(m-L-1)}{m-1} \right\rceil$. Since D is a positive integer, therefore $D \geq \frac{(m-L)(m-L-1)}{m-1}$. On solving, we get,

$$L^2 - (2m-1)L + (m-1)(m-D) \leq 0. \quad (2)$$

Let S be the discriminant of the equation

$$L^2 - (2m-1)L + (m-1)(m-D) = 0. \quad (3)$$

Then $S = 4D(m-1) + 1$. Clearly, $S > 0$. Let x_1 and x_2 be the distinct roots of the equation (3) with $x_1 < x_2$, (say). Then $L^2 - (2m-1)L + (m-1)(m-D) = (L-x_1)(L-x_2) \leq 0$. This implies that either $x_1 \leq L \leq x_2$ or $x_2 \leq L \leq x_1$. The later case is not possible since $x_1 < x_2$. Hence $x_1 \leq L \leq x_2$. Note that $x_1 = m - \frac{1}{2} - \sqrt{(m-1)D + \frac{1}{4}}$ and $x_2 = m - \frac{1}{2} + \sqrt{(m-1)D + \frac{1}{4}}$. Thus, $L \geq x_1$ gives us the desired inequality. Hence, (b) is proved.

4. Some bounds of differential uniformity of functions constructed using Lai-Massey Structure.

In this section, we explored some lower bounds of differential uniformity of $2n$ -bit function ϕ which is constructed using 3-round Lai-Massey structure with three internal n -bit S-boxes T_1 , T_2 , and T_3 as shown in Figure 1. We give some bounds on differential uniformity for S-boxes, which are constructed by the Lai-Massey structure. The input and output of the Lai-Massey structure is associated by the following equations:

$$OL(A, B) = T_2(T_1(A \oplus B) \oplus A).$$

$$OR(A, B) = T_3(T_1(A \oplus B) \oplus B),$$

where A and B are the left and right input variables, respectively, and $OL(A, B)$ and $OR(A, B)$ are the Lai-Massey structure's corresponding left and right output variables, respectively.

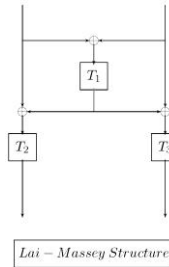


Figure 1
Lai-Massey Structures

Proposition 4.1: Let T_1, T_2 , and T_3 denote three n -bit S-boxes, and let ϕ represent the $2n$ -bit function described by the associated three-round Lai-Massey network, then

- (i) If T_3 is a permutation, then
 - (a) $|\delta_\phi(0||v, w||0)| = |\delta_{T_1}(v, v)| \times |\delta_{T_2}(v, w)|$
 - (b) $|\delta_\phi(u||u, w||z)| = |\delta_{T_2}(u, w)| \times |\delta_{T_3}(u, z)|$.
- (ii) If T_2 is a permutation, then $|\delta_\phi(u||v, 0||z)| = |\delta_{T_1}(u \oplus v, u)| \times |\delta_{T_3}(u \oplus v, z)|$.

Proof:

- (i) (a) Let $(A, B) \in \delta_\phi(0||v, w||0)$, then (A, B) be the solution of the equation (4)

$$\phi((A, B) \oplus \phi(A, B \oplus v)) = w||0 \quad (4)$$

This is equivalent to satisfy the below equations simultaneously :

$$\begin{cases} OL(A, B) \oplus OL(A, B \oplus v) &= w \\ OR(A, B) \oplus OR(A, B \oplus v) &= 0 \end{cases}$$

By solving the second equation and using the bijectivity of T_3 , we get

$$T_1(A \oplus B) \oplus T_1(A \oplus B \oplus v) = v. \quad (5)$$

Now, by expanding the initial equation, we get

$$T_2(T_1(A \oplus B) \oplus A) \oplus T_2(T_1(A \oplus B \oplus v) \oplus A) = w$$

Substituting the value of $T_1(A \oplus B \oplus v)$ from equation (5), we get

$$T_2(T_1(A \oplus B) \oplus A) \oplus T_2(T_1(A \oplus B) \oplus A \oplus v) = w$$

By putting $A \oplus B = X$ and $T_1(X) \oplus A = Y$. Since the function $(A, B) \mapsto (X, Y)$ is a bijective function, the number of (A, B) to satisfy equation (4) is equivalent to the number of (X, Y) that satisfies the pair of equations given below

$$\begin{cases} T_1(X) \oplus T_1(X \oplus v) &= v \\ T_2(Y) \oplus T_2(Y \oplus v) &= w. \end{cases}$$

Thus, we have

$$|\delta_\phi(0||v, w||0)| = |\delta_{T_1}(v, v)| \times |\delta_{T_2}(v, w)|.$$

- (b) The proof involves the same steps as in the proof of (a).
- (ii) Let T_2 be a permutation and let $(A, B) \in \delta_\phi(u||v, 0||z)$, that is, (A, B) be the solution of the equation (6).

$$\phi(A, B) \oplus \phi(A \oplus u, B \oplus v) = 0||z. \quad (6)$$

This is equivalent to saying that the pair (A, B) simultaneously satisfies the pair of equations given below.

$$\begin{cases} OL(A, B) \oplus OL(A \oplus u, B \oplus v) &= 0 \\ OR(A, B) \oplus OR(A \oplus u, B \oplus v) &= z. \end{cases}$$

By simplifying the first equation, we get

$$T_1(A \oplus B) \oplus T_1(A \oplus B \oplus u \oplus v) = u. \quad (7)$$

Similarly, by simplifying the second equation, we get

$$T_3(T_1(A \oplus B) \oplus B) \oplus T_3(T_1(A \oplus B) \oplus B \oplus u \oplus v) = z.$$

We use some notations for ease of representation as follows:

$$A \oplus B = X \text{ and } T_1(A \oplus B) \oplus B = Y.$$

By using these notations in the above equation, we get

$$T_1(X) \oplus T_1(X \oplus u \oplus v) = u \quad (8)$$

$$T_3(Y) \oplus T_3(Y \oplus u \oplus v) = z \quad (9)$$

Since the function $(A, B) \mapsto (X, Y)$ is a bijective function, the number of (A, B) to satisfy equation (6) is equivalent to the number of (X, Y) , which simultaneously satisfies equations (8) and (9). Thus we have $|\delta_\phi(u||v, 0||z)| = |\delta_{T_1}(u \oplus v, u)| \times |\delta_{T_3}(u \oplus v, z)|$.

Theorem 4.2: Let T_1, T_2 , and T_3 denote three n -bit S-boxes, and let ϕ be the $2n$ -bit function described by the associated three round Lai-Massey network. If T_3 is bijective, then

$$\Delta(\phi) \geq \max(\Delta(T_2)\Delta_{\min}(T_3), \Delta(T_3)\Delta_{\min}(T_2))$$

this can also be rewritten as follows:

$$\Delta(\phi) \geq \max_{i \neq j, i, j \neq 1} (\Delta(T_i)\Delta_{\min}(T_j)),$$

where $\Delta_{\min}(T) = \min_{a \neq 0} \max_b |\delta_T(a, b)|$.

Proof: Let $\Delta(T_2)$ is achieved at (a, c) , where $a, c \in \mathbb{F}_2^n$ be the input and output differential for S-box T_2 . Since T_3 is bijective, according to Proposition 4.1, we have

$$\Delta(T) \geq |\delta_\phi(a||a, c||d)| = |\delta_{T_2}(a, c)| \times |\delta_{T_3}(a, d)| = \Delta(T_2) \times |\delta_{T_3}(a, d)| \quad (10)$$

We can choose $d \in \mathbb{F}_2^n$ in such a way that $|\delta_{T_3}(a, d)| = \max_{b \in \mathbb{F}_2^n} |\delta_{T_3}(a, b)|$. Using equation (10) for the above value of d , we get

$$\begin{aligned} \Delta(\phi) &\geq \Delta(T_2) \times \max_{b \in \mathbb{F}_2^n} |\delta_{T_3}(a, b)| \\ &\geq \Delta(T_2) \times \Delta_{\min}(T_3). \end{aligned}$$

Similarly, we can also show $\Delta(\phi) \geq \Delta(T_3) \times \Delta_{\min}(T_2)$. Hence, we get our desired form.

$$\Delta(\phi) \geq \max(\Delta(T_2)\Delta_{\min}(T_3), \Delta(T_3)\Delta_{\min}(T_2)).$$

Corollary 4.3: Any bijective 8-bit function ϕ associated to a three-round Lai-Massey network satisfies $\Delta(\phi) \geq 8$.

Proof: Let ϕ be a bijective 8-bit function associated to a three-round Lai-Massey structure. Hence, the internal functions T_1, T_2 , and T_3 are necessarily bijective 4-bit S-boxes. Now, by Theorem 4.2, we have

$$\begin{aligned}\Delta(\phi) &\geq \max(\Delta(T_2)\Delta_{\min}(T_3), \Delta(T_3)\Delta_{\min}(T_2)) \\ &\geq \Delta(T_2)\Delta_{\min}(T_3).\end{aligned}$$

As there is no APN permutation in $\mathbb{F}_2^4$ [5] and $\Delta_{\min}(T_2) \geq 2$, this implies that, $\Delta(\phi) \geq 4 \times 2 = 8$, that is, our desired result.

5. Conclusion

This work generalize certain results of permutations differential uniformity over $\mathbb{Z}_n$ to general finite commutative ring with unity. Besides these, we have provided some bounds on the differential uniformity of functions constructed by the Lai-Massey structure. In the future, we will investigate some other cryptographic properties like non-linearity of permutations on the finite R -module M .

Conflict of Interest

Not applicable.

References

- [1] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Advances in Cryptology—EUROCRYPT'93*, Lofthus, Norway, pp. 65-76 (May 1993).
- [2] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems-CHES 2007*, Vienna, Austria, pp. 450-466 (Sep. 2007).
- [3] A. Canteaut, S. Duval, and G. Leurent, "Construction of Lightweight S-boxes Using Feistel and MISTY Structures," in *International Conference on Selected Areas in Cryptography (SAC 2015)*, Cham, Switzerland: Springer International Publishing, pp. 373-393 (Aug. 2015).
- [4] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2-3, pp. 205-244 (2004).
- [5] M. Calderini, M. Sala, and I. Villa, "A note on APN permutations in even dimension," *Finite Fields Appl.*, vol. 46, pp. 1-16 (2017).
- [6] Y. Crama and P. L. Hammer, Eds., *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, vol. 2. Cambridge, U.K.: Cambridge Univ. Press (2010).

- [7] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Amsterdam, The Netherlands: Academic Press (2017).
- [8] J. Daemen and V. Rijmen, "AES proposal: Rijndael," *Nat. Inst. Standards Technol., Comput. Security Resource Center (CSRC)* (1999).
- [9] K. Gowdhaman, T. Gulliver, C. Mohab, and D. Chinnappillai, "Con-stacyclic codes over the non-chain finite commutative ring $\mathbb{Z}_4[u,v]/\langle u^2-u, v^2, uv \rangle$," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 6, pp. 1867-1885 (2024).
- [10] P. Gupta, P. R. Mishra, and A. Gaur, "On differential uniformity and nonlinearity of permutations on $\mathbb{Z}_n$," in *Proc. 7th Int. Conf. Mathematics and Computing (ICMC 2021)*, Singapore, pp. 627-636 (2022).
- [11] P. Gupta, P. R. Mishra, and A. Gaur, "Bounds on the maximum non-linearity of permutations on the rings $\mathbb{Z}_p$ and $\mathbb{Z}_{2^p}$," *Applicable Algebra Eng. Commun. Comput.*, pp. 1-16 (2023).
- [12] Y. Kumar, P. R. Mishra, N. R. Pillai, and R. K. Sharma, "Affine equivalence and non-linearity of permutations over $\mathbb{Z}_n$," *Applicable Algebra Eng. Commun. Comput.*, vol. 28, pp. 257-279 (2017).
- [13] Y. Kumar, P. R. Mishra, and R. K. Sharma, "Nonlinearity of k-cycle permutations on $\mathbb{Z}_n$," *Asian-Eur. J. Math.*, vol. 11, no. 02, Art. no. 1850020 (2018).
- [14] Y. Li and M. Wang, "Constructing S-boxes for lightweight cryptography with Feistel structure," in *Cryptographic Hardware and Embedded Systems-CHES 2014*, pp. 127-146 (Sep. 2014).
- [15] O. A. Logachev, A. A. Salnikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptography*, vol. 241. Providence, RI, USA: Amer. Math. Soc. (2012).
- [16] P. R. Mishra, I. Gupta, and N. R. Pillai, "Non-linearity and affine equivalence of permutations," *Cryptology ePrint Archive* (2014). [Online]. Available: <https://ia.cr/2014/974>
- [17] P. R. Mishra, P. Gupta, and A. Gaur, "On full differential uniformity of permutations on the ring of integers modulo n," *Applicable Algebra Eng. Commun. Comput.*, pp. 1-19 (2021).
- [18] P. R. Mishra, Y. Kumar, N. R. Pillai, and R. K. Sharma, "On non-linearity and affine equivalence of permutations over an arbitrary finite commutative ring with unity," *Cryptologia*, vol. 42, no. 1, pp. 81-94 (2018).

- [19] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology—EUROCRYPT'93*, Lofthus, Norway, pp. 55-64 (May 1993).
- [20] G. Paul and S. Maitra, *RC4 Stream Cipher and Its Variants*. Boca Raton, FL, USA: CRC Press (2011).
- [21] B. Selikh, A. Chillali, D. Mihoubi, and N. Ghadbane, "A new public key cryptosystem based on the non-commutative ring R ," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 1, pp. 75-93 (2024).
- [22] B. Zoltak, "VMPC one-way function and stream cipher," in *Fast Software Encryption-FSE 2004*, Delhi, India, pp. 210-225 (Feb. 2004).

Received October, 2025